THE HONORABLE JOHN C. COUGHENOUR

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

PREMIER HARVEST LLC, *et al.*, Plaintiffs, v. AXIS SURPLUS INSURANCE COMPANY, *et al.*, Defendants.	CASE NO. C17-0784-JCC ORDER

This matter comes before the Court on Defendant Axis Surplus Insurance Company's motion for the Court to order David L. Anderson, dba D.L. Anderson, Inc. ("DLA"), to comply fully with Defendant's subpoena *duces tecum* (Dkt. No. 71). Having thoroughly considered the parties' briefing and the relevant record, the Court GRANTS in part and DENIES in part Defendant's motion for the reasons explained herein.

The Court has described the underlying facts of this case in previous orders and will not repeat them here. (*See* Dkt. Nos. 43, 50, 58). DLA is owned by the father of one of Plaintiffs' owners. (Dkt. No. 71.) Following Plaintiff's weather-related loss, Plaintiff engaged DLA to make emergency repairs and to provide an estimate of the repairs needed to remedy its loss-related damages. (*Id*. at 2–3.) Defendant issued a November 27, 2017 subpoena to DLA to produce documents relating to the work it performed. (*Id*. at 3); (s*ee* Dkt. No. 73-2 at 12–15)

(subpoena seeking: "All documents . . . in your possession referring or relating in any way to Premier Harvest or the property leased by Premier Harvest in Adak, Alaska."). DLA responded that it would provide what it could but it had "no remaining MS Word, Excel or photo records due to a computer virus which wiped out all of those records." (Dkt. No. 73-2 at 17.)

Defendant asked to inspect and test the affected hard drive at Defendant's cost, using an independent forensic computer specialist. (Dkt. No. 71 at 4.) This would involve cloning the hard drive and sending the cloned version off-site for analysis and file recovery. (*Id*.) Recovered files could then be sent directly to DLA for review. (*Id*.) DLA would determine which files were responsive to the subpoena, and produce those files, unless DLA determined such files were subject to privilege or protection. (*Id*.)

Following Defendant's proposal and further discussions between DLA and Defendant's counsel, DLA indicated that it had located a backup of the hard drive at issue and concluded "it seems we can satisfy the requirements of the subpoena" without providing the infected hard drive for cloning. (Dkt. No. 73-2 at 188.) DLA further indicated that if this approach did not satisfy Defendant, DLA would allow "an agreed upon independent computer specialist to copy [files off the infected hard drive] . . . but that must be done in my office and they would only be allowed to copy and remove [responsive documents] . . . [the independent computer specialist] would not be allowed to remove entire copies of the hard drive." (Dkt. No. 73-2 at 188.)

Defendant's counsel indicated to DLA that responsive files from the backup would satisfy the subpoena, so long as DLA's computer specialist signed a written statement indicating the backup DLA had located contained "all information that was damaged or lost on the laptop as a result of the virus." (*Id*. at 194.) Absent such a declaration, there is no way of knowing whether DLA has, in fact, located and provided all responsive documents from the infected hard drive. Defendant contends that, absent the attestation described above, DLA's conditions would not satisfy the subpoena because the *entire* affected hard drive—not just responsive documents that can be recovered on-site— must be cloned and sent off-site to ensure that all potentially-

recoverable responsive files are, in fact, recovered. (Dkt. No. 73-2 at 183); (*see* Dkt. No. 72 at 2–3) (forensic computer specialist's declaration describing the recovery process and the need for off-site access to the entire hard drive).

DLA has since provided Defendant a flash drive containing what DLA contends are "all pertinent Premier Harvest emails and documents from the back up files." (Dkt. No. 87-1 at 5.) But DLA has not provided an attestation that the backup it located contained all of the files from the infected hard drive. (*Id*. at 5–6.)

Defendant seeks an order that DLA fully comply with the subpoena, and if DLA cannot verify that all information stored on the infected hard drive is available via back up files, Defendant seeks an order that DLA provide Defendant's forensic computer specialist access to the laptop and hard drive at issue, and that DLA produce all responsive documents within ten days of the specialist's evaluation of the hard drive. (*See generally* Dkt. No. 71.)

Absent undue burden or cost, or claims of privilege or protection, a person served with a subpoena *duces tecum* for documents and electronically stored information must produce that information. Fed. R. Civ. P. 45(e). If the recipient fails to do so, or to timely object, the party serving the subpoena may seek an order to compel the recipient to produce the documents or to furnish for inspection the files containing the documents. Fed. R. Civ. P. 45(d)(2)(B)(i). A person who fails comply with a court order to produce documents may be held in contempt. Fed. R. Civ. P. 45(f); *Pennwalt Corp. v. Durand-Wayland, Inc.*, 708 F.2d 492, 495 (9th Cir. 1983).

Absent an affidavit from DLA that the backup files it located contain all the information from the infected hard drive, Defendant has no assurance that DLA has provided all potentially-available responsive files. Defendant's suggested approach—having an independent forensic computer specialist clone the entire affected hard drive, send it off-site for analysis, and provide all recovered files to DLA for review before responding to the subpoena—is reasonable. But the Court emphasizes that the forensic computer specialist Defendant contracts with must be independent of Defendant. Based on the declaration provided by Kevin M. Hecksher, the Court

concludes that Mr. Hecksher is an independent forensic computer specialist. (*See* Dkt. No. 72 at 1–9.)

For the foregoing reasons, Defendant's motion to compel (Dkt. No. 71) is GRANTED in part and DENIED in part. DLA is ORDERED to either:

(1) Provide Defendant within seven (7) days:

a. a signed attestation from its computer specialist that all information stored on the virus-infected hard drive is available by means of backup files, *and*

b. a signed attestation from a DLA representative that it reviewed those back up files and provided all responsive files to Defendant in the thumb drive referenced in Dave Anderson's March 6, 2018 e-mail to Craig Bennion; ***or***

(2) Provide Mr. Hecksher, or another independent forensic computer specialist if Mr. Hecksher is unavailable, within seven (7) days:

a. access to clone the entire infected hard drive, *and*

b. upon DLA's receipt of recovered files, DLA must provide, within ten (10) days of receipt of recovered files, all responsive files to Defendant.

Any privilege or protection DLA seeks to assert relating to responsive documents must be made in accordance with Federal Rule of Civil Procedure 45(e)(2).

DATED this 23rd day of March 2018.

John C. Coughenour
UNITED STATES DISTRICT JUDGE